Ohne Cybersicherheit keine Marktzulassung

Wie Unternehmen den CRA erfolgreich umsetzen

Der neue Cyber Resilience Act wird Voraussetzung für die Vergabe des „CE" Zeichens, damit dürfen Geräte mit Cyber-Schwachstellen in der EU nicht mehr verkauft werden.

Autor:
Jan Wendenburg
CEO
ONEKEY
https://onekey.com/

Der Cyber Resilience Act (CRA) der Europäischen Kommission, der am 10. Dezember 2024 verabschiedet wurde und mit einer Übergangsfrist in Kraft treten wird, stellt die bisher umfassendste Regelung zur Cybersicherheit vernetzter Produkte in Europa dar. Für die Hersteller von Embedded-Systemen sowie Geräten für das Internet of Things (IoT) und das Industrial IoT drängt die Zeit, denn die neuen Sicherheitsvorgaben müssen bereits bei der Entwicklung berücksichtigt werden (Security by Design). Die ersten Vorschriften finden ab September 2026 und alle restlichen ab dem 11. Dezember 2027 Anwendung. Ab diesem Zeitpunkt müssen alle vernetzten Produkte die Cybersicherheitsanforderungen des Cyber Resilience Act vollständig erfüllen. Hersteller, Importeure und Händler sind gefordert: Ohne CRA-Konformität dürfen die betroffenen Produkte nicht mehr in der EU verkauft werden. Die Meldepflicht für Sicherheitslücken greift sogar schon ab dem 11. September 2026. Angesichts von Produktlebenszyklen von in der Regel vielen Jahren sollte dem Thema CRA also höchste Priorität eingeräumt werden, um auch künftig auf dem EU-Markt verkaufen zu können.

Zentrale Elemente der CRA-Compliance

Zentrale Elemente für die CRA-Compliance sind das Prinzip „Security by Design" sowie eine kontinuierliche Risikobewertung und Schwachstellenbehebung. Darüber hinaus wird eine Software Bill of Materials (SBOM) gefordert, um Softwarekomponenten rückverfolgbar zu machen und Risiken in der Lieferkette frühzeitig zu erkennen. Der CRA kategorisiert Produkte in drei Sicherheitsklassen und definiert verbindliche Anforderungen für Consumer IoT, Industrial IoT-Anwendungen und Embedded Systems. Die Sicherheit der Lieferkette ist besonders relevant, da Schwachstellen in Drittanbieter- und Open-Source-Komponenten die Integrität des Gesamtsystems gefährden können. Die Umsetzungsfrist von 24, bzw. 36 Monaten seit Inkrafttreten am 10. Dezember 2024 stellt Hersteller vor große Herausforderungen, da Produktentwicklungen oft Jahre dauern.

Best Practices zur Cybersicherheit

Um den Anforderungen des CRA gerecht zu werden, sollten Unternehmen schnellstmöglich Best Practices zur Cybersicherheit implementieren. Dabei gilt es, neben dem CRA weitere regulatorische Rahmenbedingungen wie RED II und IEC 62443 zu berücksichtigen. Spezielle Compliance Tools können helfen, die heutigen und künftigen Anforderungen zu erfüllen, indem sie eine effiziente Cybersicherheitsbewertung von Produkten ermöglichen.

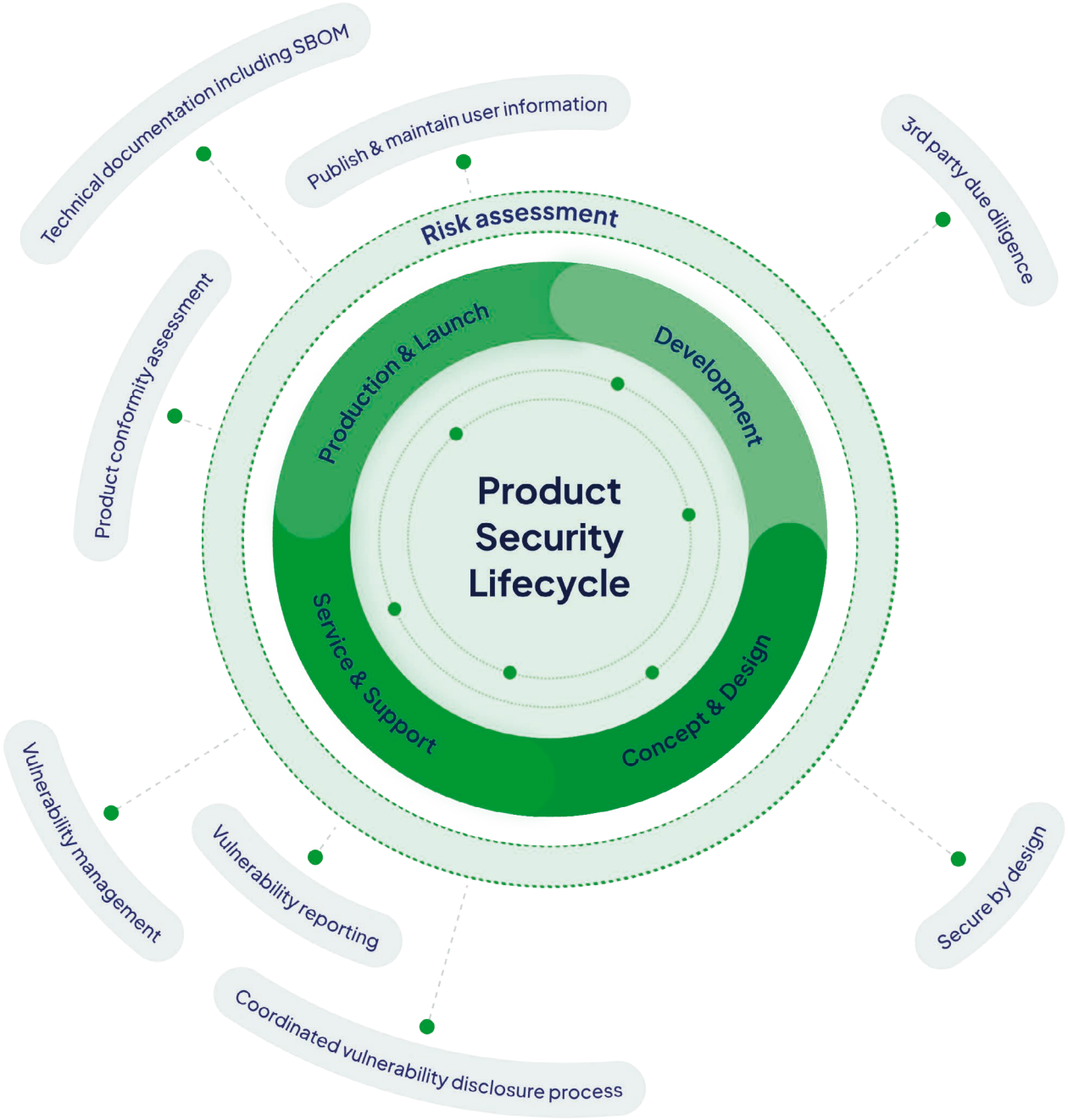
Unternehmen, die ihre Produktstrategie rechtzeitig anpassen, sichern nicht nur ihre Marktzulassung in der EU, sondern auch ihre Wettbewerbsfähigkeit. Lifecycle Security, proaktive Compliance und Supply Chain Security werden zu zentralen Erfolgsfaktoren für die Hersteller auf dem Markt.

Neue Anforderungen des CRA und ihre Auswirkungen

Vernetzte Produkte aller Art müssen künftig eine Reihe neuer Sicherheitsanforderungen erfüllen, um das CE-Zeichen (Conformité Européenne) zu erhalten, das bescheinigt, dass sie den Vorschriften der Europäischen Union entsprechen. Dies betrifft alle Geräte, Maschinen und Komponenten, die digitale Technologien nutzen oder eine direkte oder indirekte Verbindung zu anderen Geräten oder Netzwerken herstellen. Ohne das CE-Zeichen dürfen diese Produkte in der EU nicht verkauft oder vertrieben werden. Und dabei spielt der CRA künftig eine Schlüsselrolle.

Pflichten der Hersteller

Der CRA verpflichtet alle Hersteller zur regelmäßigen Prüfung, Überwachung und Dokumentation der Cybersicherheit ihrer Produkte. Um den neuen Anforderungen gerecht zu werden, sollten Unternehmen in



der Lage sein, Sicherheitslücken schnell zu erkennen und ein kontinuierliches Impact Assessment durchzuführen. Das bedeutet, dass jede Schwachstelle laufend bewertet werden muss, um die Produkte gründlich zu analysieren und sich vor potenziell schwerwiegenden Auswirkungen von Sicherheitslücken zu schützen.

Der CRA verlangt nicht nur von Herstellern, sondern auch von Importeuren und Händlern, für die Sicherheit der Produkte zu sorgen. Ziel des Gesetzgebers ist es, die gesamte digitale Lieferkette innerhalb des EU-Binnenmarktes abzusichern. Cybersicherheit wird dadurch zu einer entscheidenden Voraussetzung für den Zugang zum europäischen Markt.

Im Vergleich zu Standards wie RED II und IEC 62443 geht der CRA einen Schritt weiter, indem er konkrete und verbindliche Anforderungen an die Cybersicherheit vernetzter Produkte festlegt. Während RED II und IEC 62443 bereits wichtige Sicherheitsaspekte in spezifischen Bereichen wie Telekommunikation und Industrieautomation abdecken, stellt der CRA ein deutlich umfassenderes Regelwerk dar, das die Sicherheit digitaler Produkte auf europäischer Ebene stärken soll.

Lifecycle Security

Cybersicherheit über den gesamten Produktlebenszyklus: Die CRA-Vorgaben betreffen den gesamten Lebenszyklus der betroffenen Produkte – von der Planung und Entwicklung bis hin zum Betrieb und der anschließenden Außerbetriebnahme. Hersteller sind verpflichtet, Sicherheitsupdates für ihre Produkte über einen Zeitraum von mindestens fünf Jahren anzubieten. Sollte die Nutzung des Produkts kürzer sein, kann dieser Zeitraum entsprechend verkürzt werden. In vielen Industriebereichen jedoch sind Produktlaufzeiten von 10 oder 20 Jahren oder sogar länger keine Seltenheit. Das bedeutet, dass auch die Überwachung, Wartung, das Schwachstellenmanagement und die Patch-Strategien über einen entsprechend langen Zeitraum aufrechterhalten werden müssen.

Unterschiedliche Betriebssysteme

Im Kontext der Cybersicherheit und des Cyber Resilience Acts spielen unterschiedliche Betriebssysteme eine zentrale Rolle.

Echtzeitbetriebssysteme (Real-time Operating Systems, RTOS) zeichnen sich durch ihre Fähigkeit aus, auf zeitkritische Anforderungen zu reagieren, was sie besonders für Embedded Systems, IoT und IIoT geeignet macht. Sie bieten eine präzise Steuerung und schnelle Reaktionszeiten, was in sicherheitskritischen Anwendungen von großer Bedeutung ist.

Im Gegensatz dazu bietet Linux als Open-Source-Betriebssystem eine breite Flexibilität und wird aufgrund seiner Stabilität und Anpassungsfähigkeit oft in der Entwicklung komplexer Anwendungen und IoT-Geräte eingesetzt. Während Linux eine umfangreiche Entwicklergemeinschaft und regelmäßige Sicherheitsupdates bietet, können RTOS durch eingeschränkte Funktionalität und geringe Angriffsfläche in sicherheitskritischen Umgebungen Vorteile bieten. Andere Systeme, wie proprietäre Betriebssysteme, haben oft spezifische Vor- und Nachteile, insbesondere in Bezug auf den Support und die Sicherheitsfeatures, die sie bieten. In Bezug auf den CRA müssen Unternehmen sicherstellen, dass alle eingesetzten Systeme, unabhängig vom Typ, den neuen Sicherheitsanforderungen gerecht werden. Eine Schlüsselrolle spielt dabei die Software Bill of Materials (SBOM).

Supply Chain Security:

Transparenz und Schutz vor Manipulationen: Hersteller von „Produkten mit digitalen Elementen" sind im Rahmen der Dokumentationspflicht des Cyber Resilience Act künftig dazu verpflichtet, eine Software Bill of Materials (SBOM) zu führen und die gesamte Lieferkette auf Sicherheitsrisiken zu überprüfen. Diese Regelung betrifft eine breite Palette von Geräten – von Laptops, Smartwatches und Smart-Home-Systemen wie intelligenten Thermostaten oder Stromzählern bis hin zu industriellen Steuerungen und vernetzten Fahrzeugen. Kurz gesagt: Alle IT- oder internetfähigen Produkte fallen darunter.

Die SBOM

ist eine digitale Stückliste, die sämtliche in einem Produkt verwendeten Softwarekomponenten – auch die nicht direkt offensichtlichen – auflistet. Hersteller, Importeure und Händler müssen sicherstellen, dass diese Liste stets aktuell bleibt. Jede Softwareaktualisierung oder Sicherheitskorrektur erfordert daher eine kontinuierliche Pflege der SBOM, idealerweise durch einen automatisierten Prozess. Mit automatischen Compliance Tools lässt sich die SBOM erstellen, überwachen und fortlaufend aktualisieren, sodass Unternehmen jederzeit über eine präzise und konforme Dokumentation verfügen.

Außerdem müssen Hersteller dafür sorgen, dass ihre Lieferketten vor Manipulationen geschützt sind. Die zunehmende Vernetzung von Produkten macht es für Cyberkriminelle einfacher, Angriffe über Schwachstellen in der Lieferkette durchzuführen. Um dies zu verhindern, müssen Unternehmen auf Transparenz setzen und sicherstellen, dass sämtliche Komponenten und Softwarequellen überprüft und dokumentiert werden. Dies schützt nicht nur vor potenziellen Sicherheitslücken, sondern stellt auch sicher, dass alle Produktbestandteile den regulatorischen Anforderungen entsprechen, was für den Marktzugang in der EU unerlässlich ist.

Viele Herausforderungen

Die Umsetzung des Cyber Resilience Act stellt Hersteller vor erhebliche praktische Herausforderungen. Ein Beispiel hierfür ist die Industrielle Fertigung, in der industrielle Steuerungs- und Produktionsanlagen über Jahrzehnte genutzt werden und regelmäßige Sicherheitsupdates erforderlich sind, um die Konformität zu gewährleisten. In der IoT-Industrie, etwa bei smarten Haushaltsgeräten, ist die ständige Pflege der Software Bill of Materials ebenfalls notwendig, um potenzielle Schwachstellen schnell zu identifizieren und zu beheben. Unternehmen müssen daher mit ihren Zulieferern eng zusammenarbeiten, um eine lückenlose Sicherheitsüberwachung über den gesamten Lebenszyklus des Produkts hinweg zu gewährleisten. Automatisierte Prozesse zur Schwachstellenanalyse und -behebung sind hierbei unerlässlich, um die Anforderungen effizient zu erfüllen und gleichzeitig Ressourcen zu schonen.

CRA als Wettbewerbsvorteil

Compliance & Marktanforderungen: Die frühzeitige Umsetzung der Anforderungen des Cyber Resilience Act bietet Unternehmen einen erheblichen Wettbewerbsvorteil. Durch die proaktive Integration von Cybersicherheitsmaßnahmen und die Sicherstellung der Compliance können Unternehmen nicht nur rechtliche und finanzielle Risiken minimieren, sondern sich auch als vertrauenswürdige Partner auf dem Markt positionieren. In einer Zeit, in der Verbraucher und Geschäftspartner zunehmend Wert auf Datensicherheit legen, schafft die Einhaltung des CRA ein starkes Vertrauen, das die Markenreputation stärkt. Zudem verschaffen sich Unternehmen, die frühzeitig in Sicherheitslösungen investieren, einen strategischen Vorteil gegenüber Wettbewerbern, die erst später auf die neuen Anforderungen reagieren. Die proaktive Anpassung an gesetzliche Vorgaben fördert also nicht nur den Marktzugang in der EU, sondern verbessert auch die langfristige Marktstellung, da Unternehmen als Vorreiter in der Sicherheitswahrnehmung gelten.

Best Practices

So setzen Hersteller die CRA-Anforderungen erfolgreich um: Um die Anforderungen des CRA erfolgreich umzusetzen, sollten Hersteller auf bewährte Best Practices setzen. Sicherheitsanforderungen sollten frühzeitig in den Produktentwicklungsprozess integriert und regelmäßige Sicherheitsbewertungen durchgeführt werden. Unternehmen sind gut beraten, ihre Lieferketten zu überprüfen und sicherzustellen, dass Zulieferer und Partner die geforderten Sicherheitsstandards einhalten.

Monitoring und Patchen

Ein Monitoring und Patchen von Sicherheitslücken während des Produktlebenszyklus ist unerlässlich, um die CRA-Konformität sicherzustellen. Hersteller sollten transparente Kommunikationskanäle mit Regulierungsbehörden und Kunden pflegen, um Vertrauen aufzubauen.

Compliance Tools

unterstützen Hersteller, Importeure und Händler von Produkten mit digitalen Komponenten bei der Einhaltung von Sicherheitsvorgaben. Sie ermöglichen eine umfassende Cybersicherheitsbewertung, indem sie automatische Schwachstellenerkennung, CVE-Priorisierung und intelligente Filterung mit einer interaktiven, ganzheitlichen Compliance-Überprüfung kombinieren. Dadurch lassen sich die Komplexität sowie die Kosten von Cybersicherheits- und Konformitätsprozessen signifikant reduzieren.

Automatisierte Compliance-Dienste

Der Cyber Resilience Act stellt die Firmen vor erhebliche Herausforderungen – wird aber sicherlich noch nicht das Ende sein. Weitere und noch strengere Anforderungen an die Cybersecurity sind abzusehen und angesichts der sich verschärfenden Bedrohungslage zweifelsohne auch gerechtfertigt. Die Unternehmen vernetzter Produkte sind daher gut beraten, in Sachen Produkt Cybersicherheit soweit wie möglich auf automatisierte Compliance-Dienste zu setzen. Künftige Entwicklungen könnten noch detailliertere Anforderungen an Transparenz, Reaktionsfähigkeit auf Sicherheitsvorfälle und die Verantwortung von Lieferanten mit sich bringen. Unternehmen, die sich frühzeitig auf diese Veränderungen einstellen, erfüllen nicht nur die regulatorischen Anforderungen, sondern verschaffen sich auch einen Wettbewerbsvorteil und stärken ihre Marktposition.

Fazit

Die Anforderungen des Cyber Resilience Act stellen Hersteller vor neue Herausforderungen, die jedoch gleichzeitig Chancen bieten, durch proaktive Cybersicherheit einen Wettbewerbsvorteil zu erzielen. Strengere regulatorische Vorgaben und die zunehmende Bedeutung der Cybersicherheit erfordern, dass Unternehmen jetzt handeln, um Compliance-Risiken zu minimieren und den Marktzugang in der EU zu sichern. Hersteller sollten sofort mit der Integration von Sicherheitsmaßnahmen in ihre Produktentwicklung beginnen, ihre Lieferketten überprüfen und kontinuierliche Sicherheitsüberwachung sicherstellen. Durch diese Schritte können sie nicht nur gesetzliche Anforderungen erfüllen, sondern auch ihre Position als vertrauenswürdiger Marktakteur stärken. ◄